PRBIT - Princípy bezpečnosti informačných technológií

Report - Domáca úloha č.8

Autor: Marek Čederle

Cvičenie: Pondelok 17:00

Použité príkazy a ich vysvetlenie

Zadanie č.4

Prihláste sa ako Administrátor

1. Na disku C: vytvorte priečinok UDAJE
2. V priečinku UDAJE vytvorte priečinky FINANCNE a PERSONALNE
3. V jednotlivých priečinkoch vytvorte ľubovoľný textový súbor s ľubovoľným obsahom.
4. Vytvorte používateľa user2 rovnako ako ste vytvorili používateľa nesúceho Vaše krstné meno
5. Vytvorte globálne používateľské skupiny Finančné oddelenie a Personálne oddelenie
6. Zaraďte používateľa:
    a. Vaše krstné meno do skupiny Finančné oddelenie
    b. User2 do skupiny Personálne oddelenie
7. Prostredníctvom nastavenia oprávnení na úrovni súborového systému nastavte, aby
    a. Do priečinku UDAJE mohli čítať a zapisovať do daného priečinka, všetkých podpriečinkov Administrátori servera
    b. Obsah priečinka UDAJE si mohli ZOBRAZIŤ používatelia zo skupín Finančné a Personálne oddelenie
    c. Obsah priečinka FINANCNE si mohol zobraziť a upravovať iba používateľ v skupine Finančného oddelenia
    d. Obsah priečinka PERSONALNE si mohol zobraziť a upravovať iba používateľ v skupine Personálneho oddelenia
8. Správnosť svojho riešenia dokumentujte skúškou:
    a. Z konta administrátor prehliadať obsah všetkých priečinkov vytvorených v tejto úlohe + zapisovať do nich
    b. Z konta Vaše krstné meno sa pokúsiť zobraziť obsah priečinka PERSONALNE a dokumentovať chybovú hlášku - printscreen, ktorá sa objaví
    c. Z konta user2 sa pokúsiť zobraziť obsah priečinka FINANCNE a dokumentovať ako v kroku b.
    d. Z kont Vaše krstné meno a user2 skúsiť zapisovať do priečinka UDAJE
    e. Z kont Vaše krstné meno a user2 skúšať zapisovať do priečinkov, do ktorých majú práva zápisu

1. plus 2. Vytvorenie daných adresárov:

```
mkdir C:\UDAJE
mkdir C:\UDAJE\FINANCNE
mkdir C:\UDAJE\PERSONALNE
```

3.

Vytvorenie súborov:

```
notepad financne.txt
```

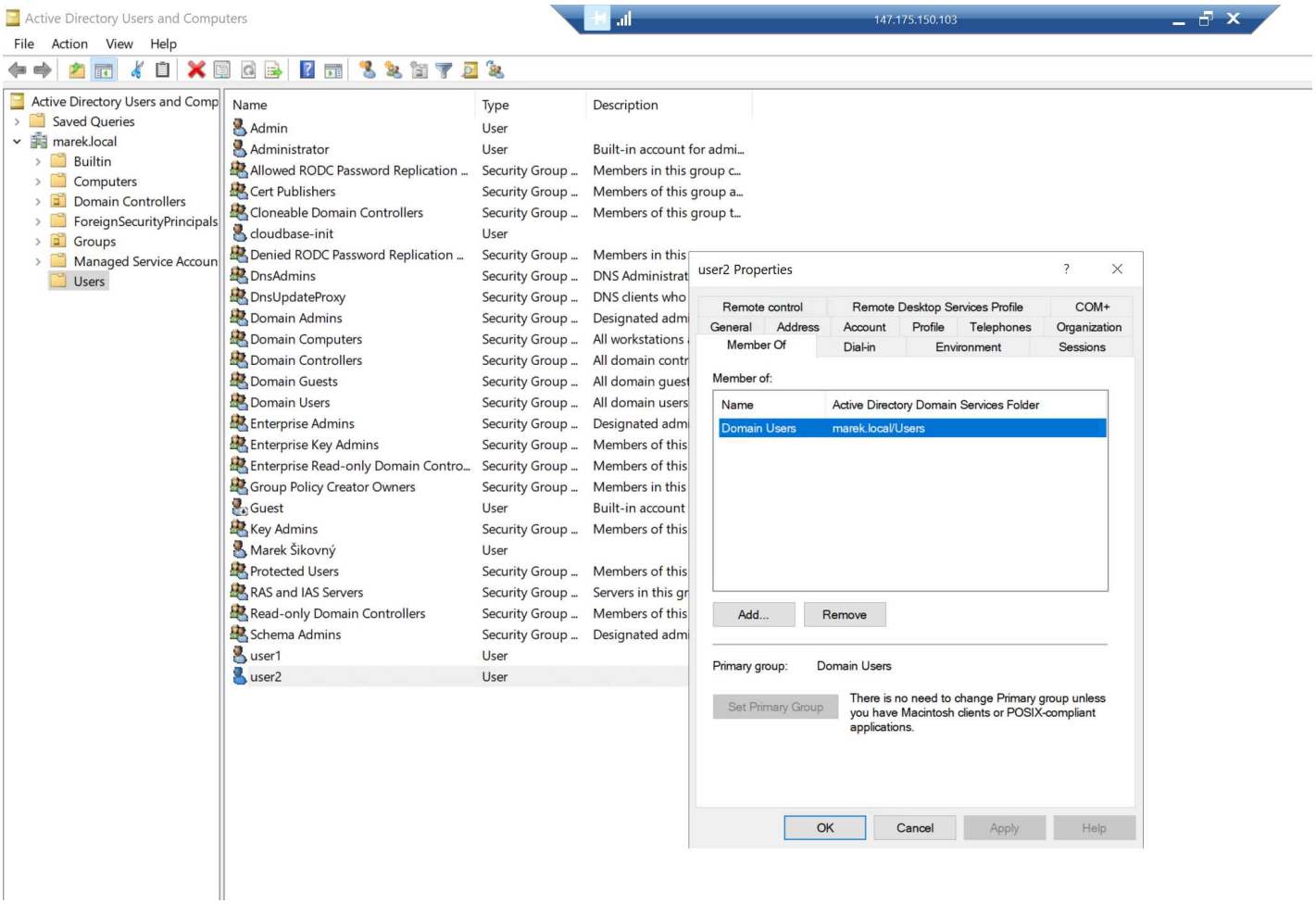
- napísal som tam text `financne test test`

```
notepad personalne.txt
```

- napísal som tam text `personalne test test`

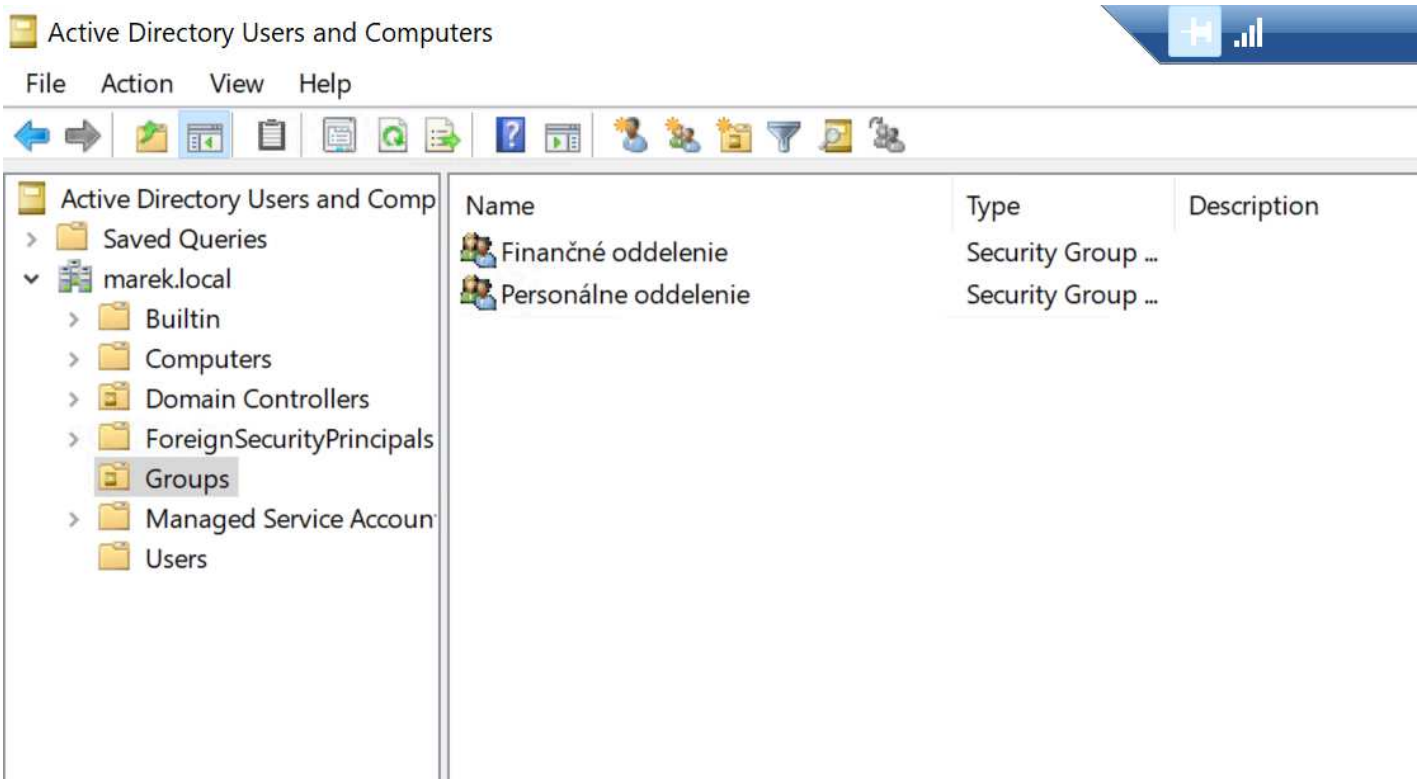
4.

Pridanie `user2` ako doménového používateľa:



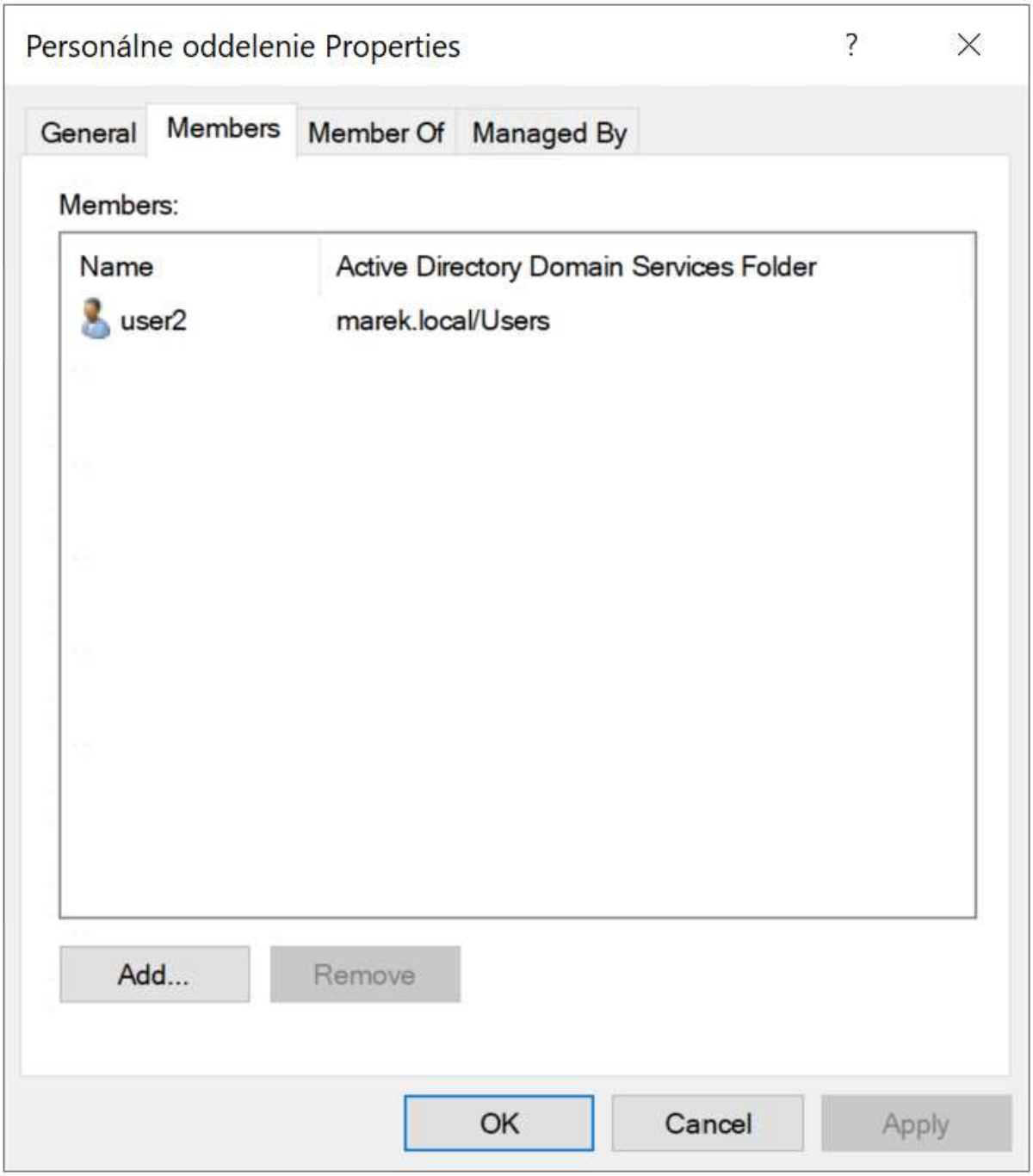
5.

Vytvorenie skupin:



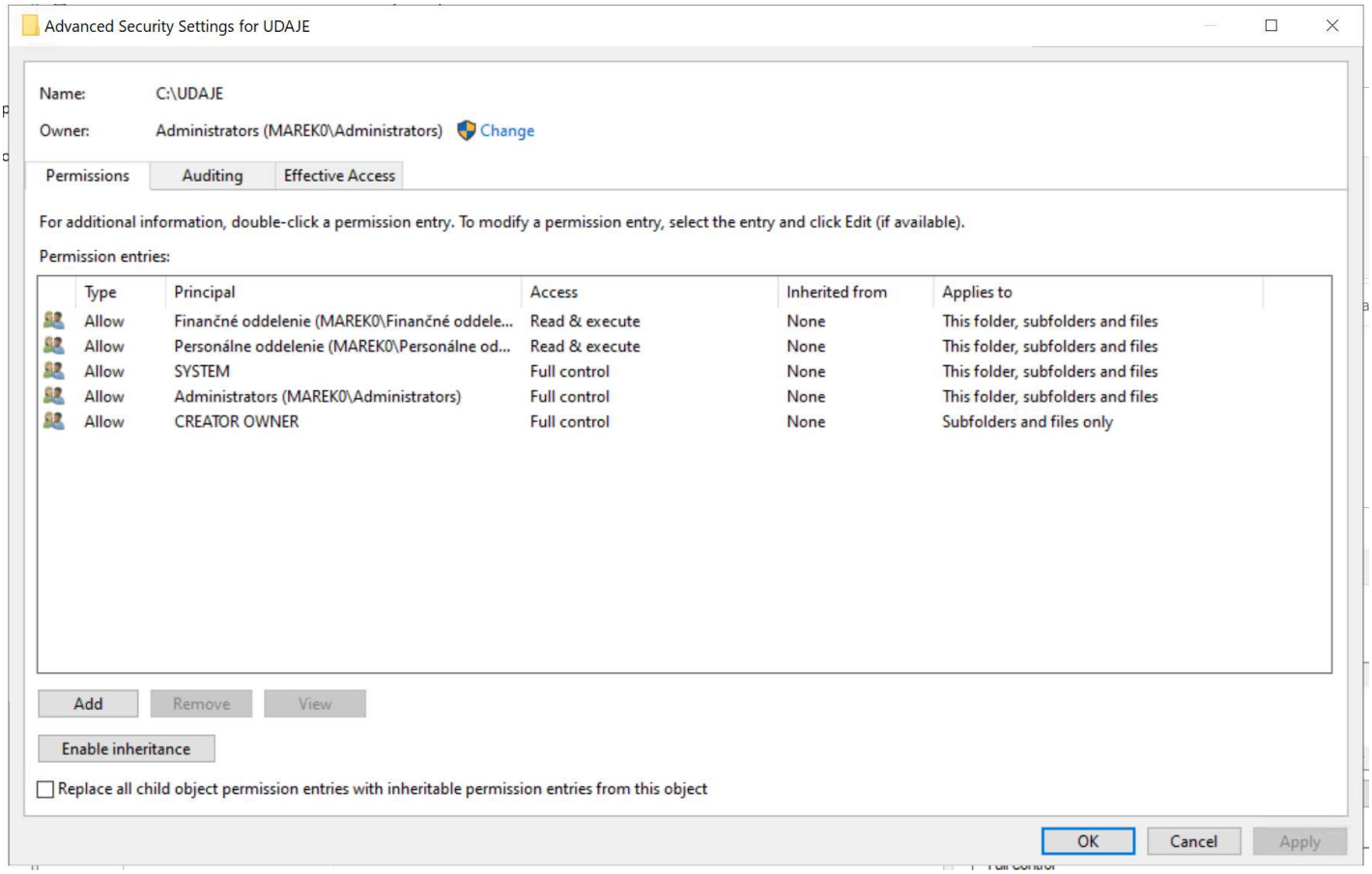
6.

Pridanie používateľov do ich špecifikovaných skupín (ukážka iba toho druhého, ale prvý je dobre nastavený):

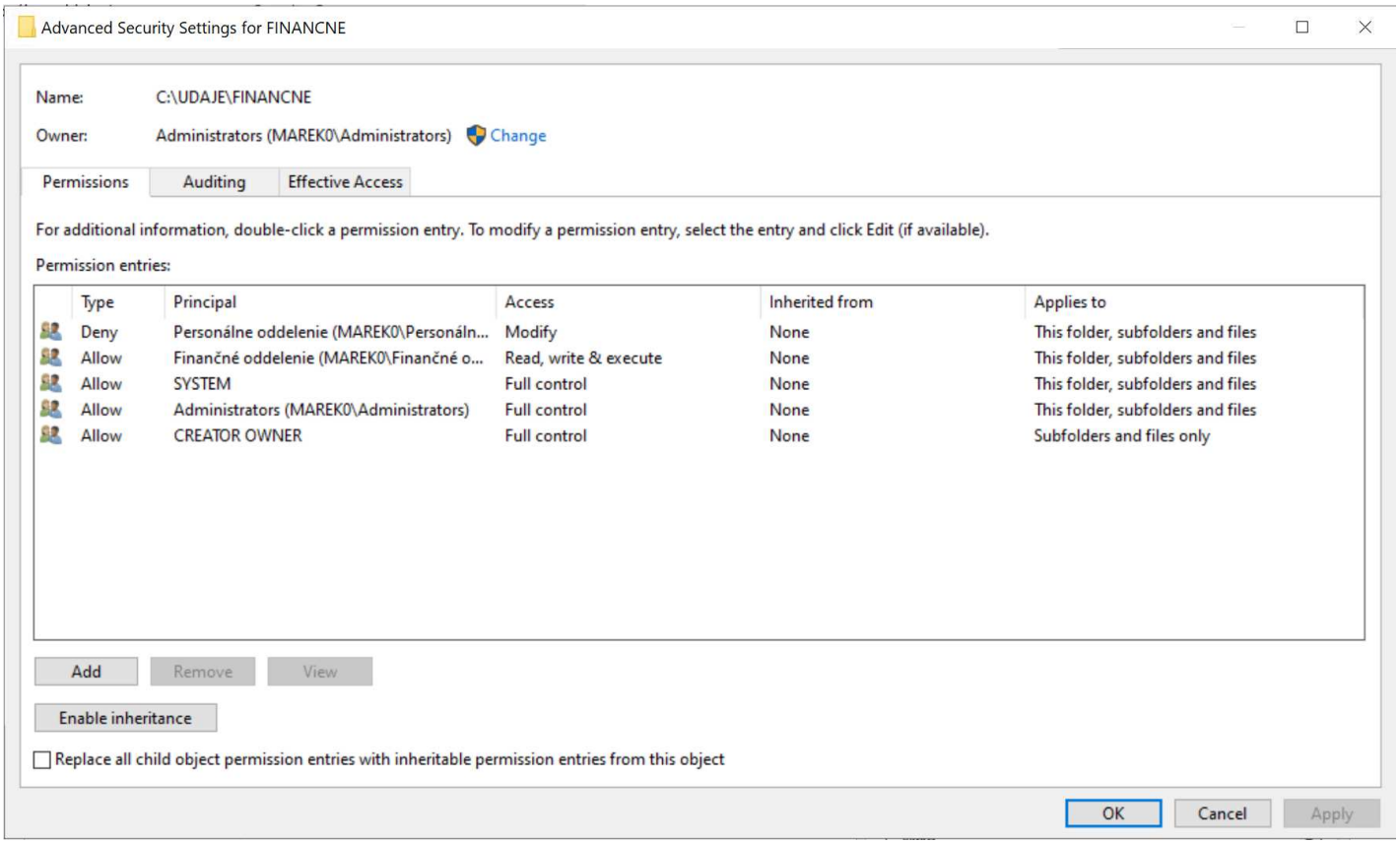


7.

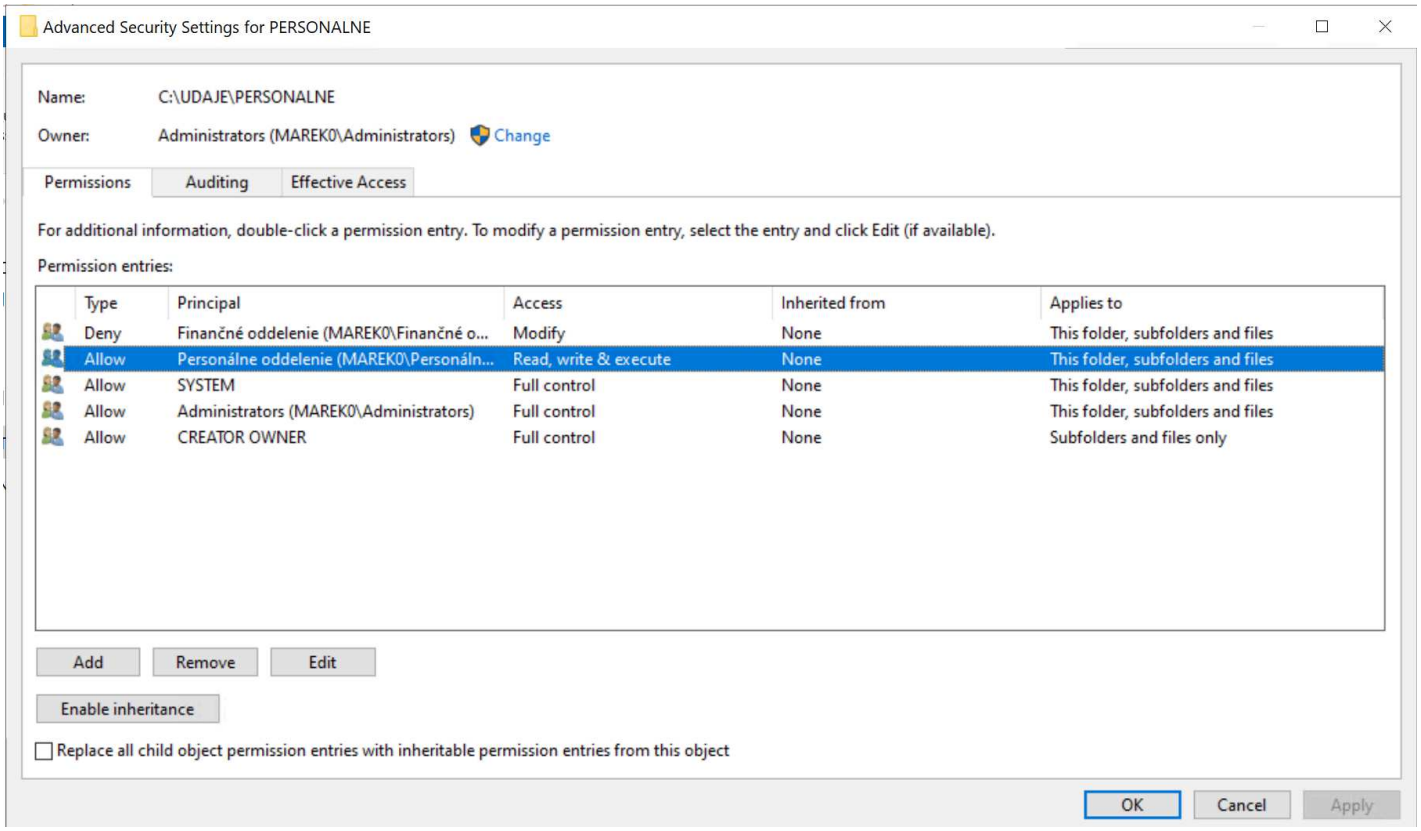
Povolenia pre priečinok `UDAJE`:



Povolenia pre priečinok `FINANCNE`:



Povolenia pre priečinok `PERSONALNE`:

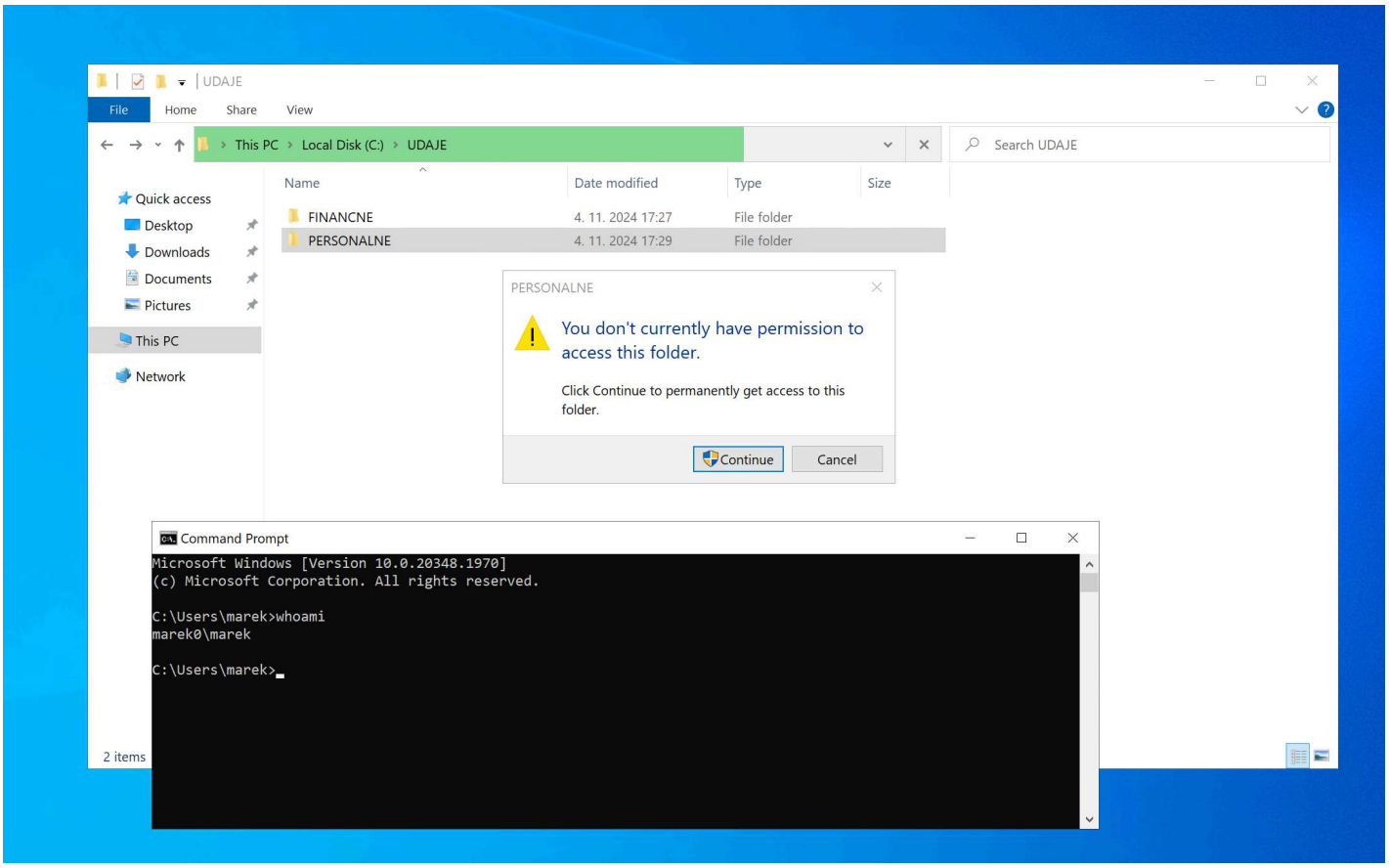


8.

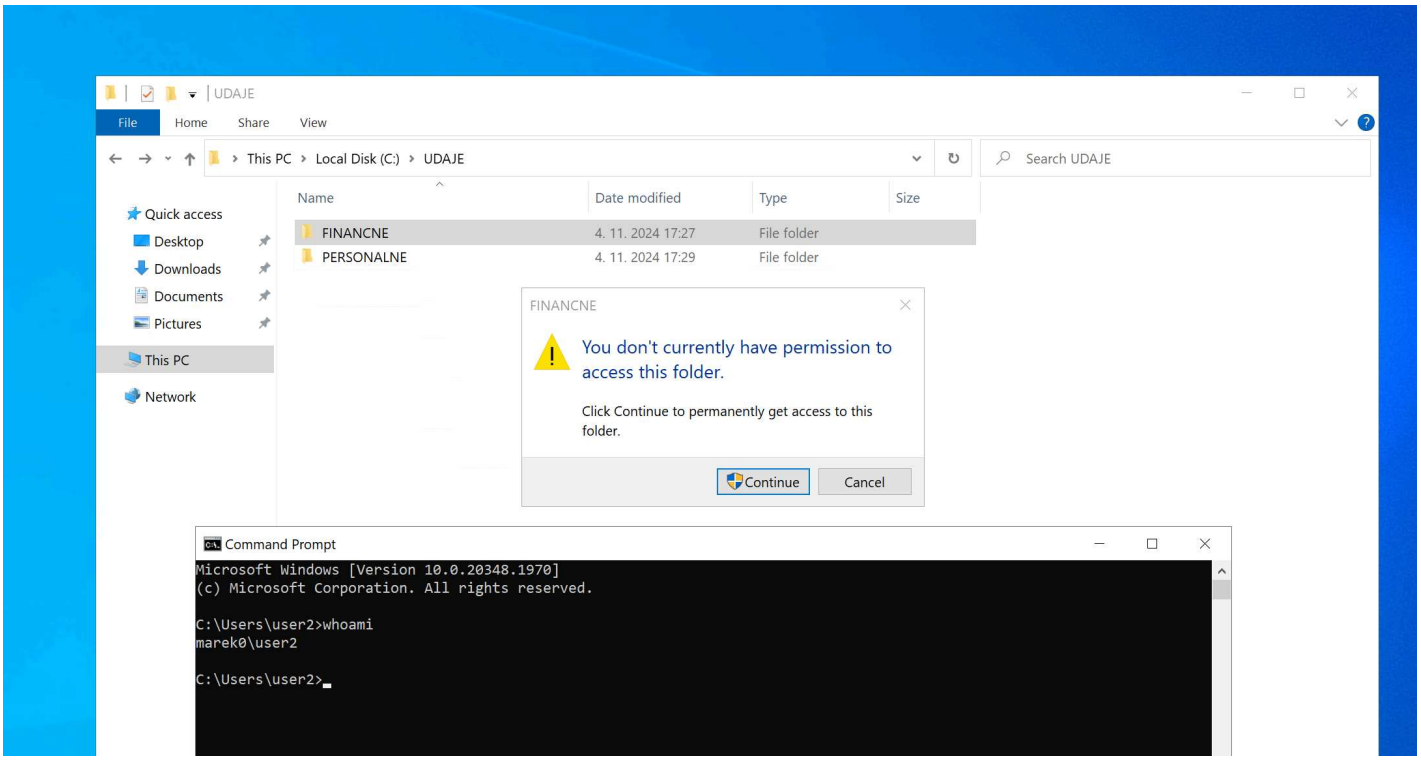
a)

- Ako (prihlásený) admin som to vedel otvoriť a upravit.

b)


UDAJE
File
Home
Share
View
This PC
Local Disk (C:)
UDAJE
Search UDAJE
Quick access
Desktop
Downloads
Documents
Pictures
This PC
Network
Name
Date modified
Type
Size
FINANCNE
4. 11. 2024 17:27
File folder
PERSONALNE
4. 11. 2024 17:29
File folder
PERSONALNE
You don't currently have permission to access this folder.
Click Continue to permanently get access to this folder.
Continue
Cancel
Command Prompt
Microsoft Windows [Version 10.0.20348.1970]
(c) Microsoft Corporation. All rights reserved.
C:\Users\marek>whoami
marek0\marek
C:\Users\marek>
2 items

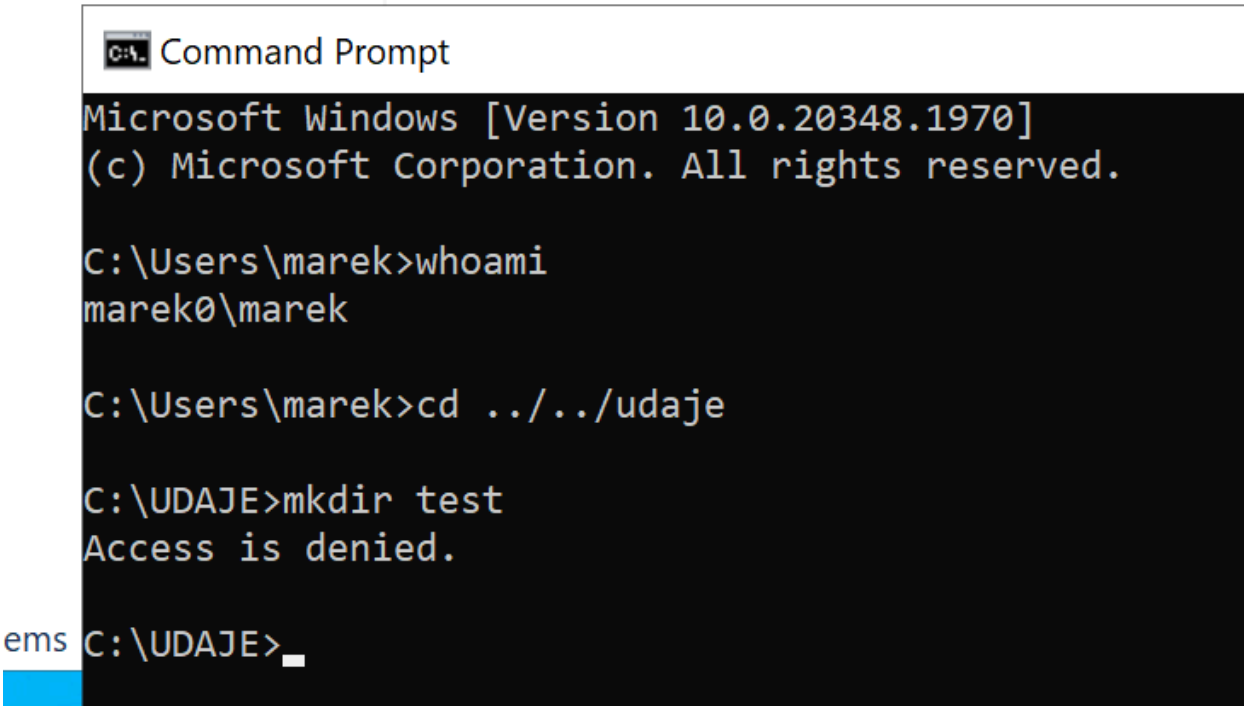
c)


UDAJE
File
Home
Share
View
This PC
Local Disk (C:)
UDAJE
Search UDAJE
Quick access
Desktop
Downloads
Documents
Pictures
This PC
Network
Name
Date modified
Type
Size
FINANCNE
4. 11. 2024 17:27
File folder
PERSONALNE
4. 11. 2024 17:29
File folder
FINANCNE
You don't currently have permission to access this folder.
Click Continue to permanently get access to this folder.
Continue
Cancel
Command Prompt
Microsoft Windows [Version 10.0.20348.1970]
(c) Microsoft Corporation. All rights reserved.
C:\Users\user2>whoami
marek0\user2
C:\Users\user2>

d)

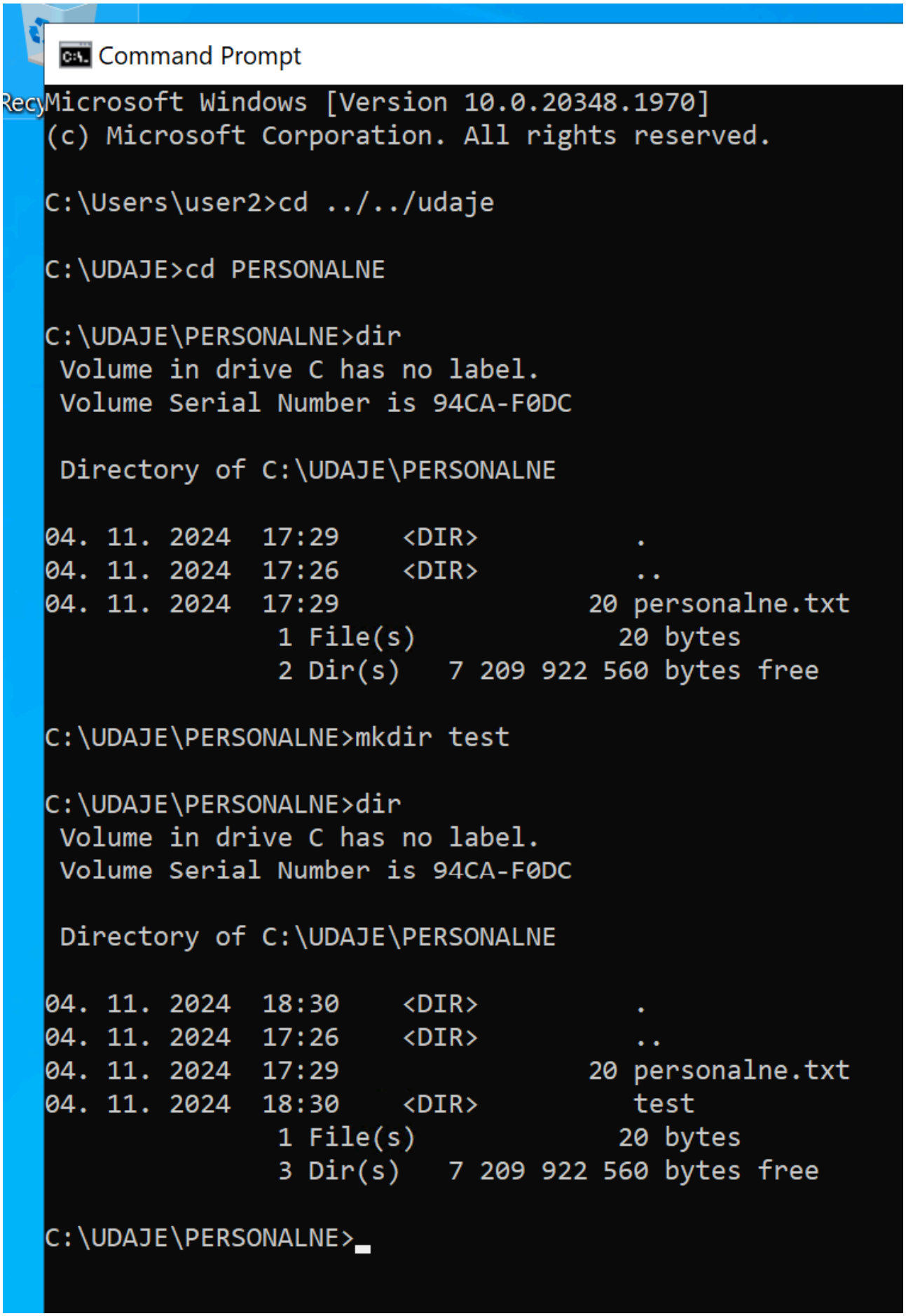
Command Prompt

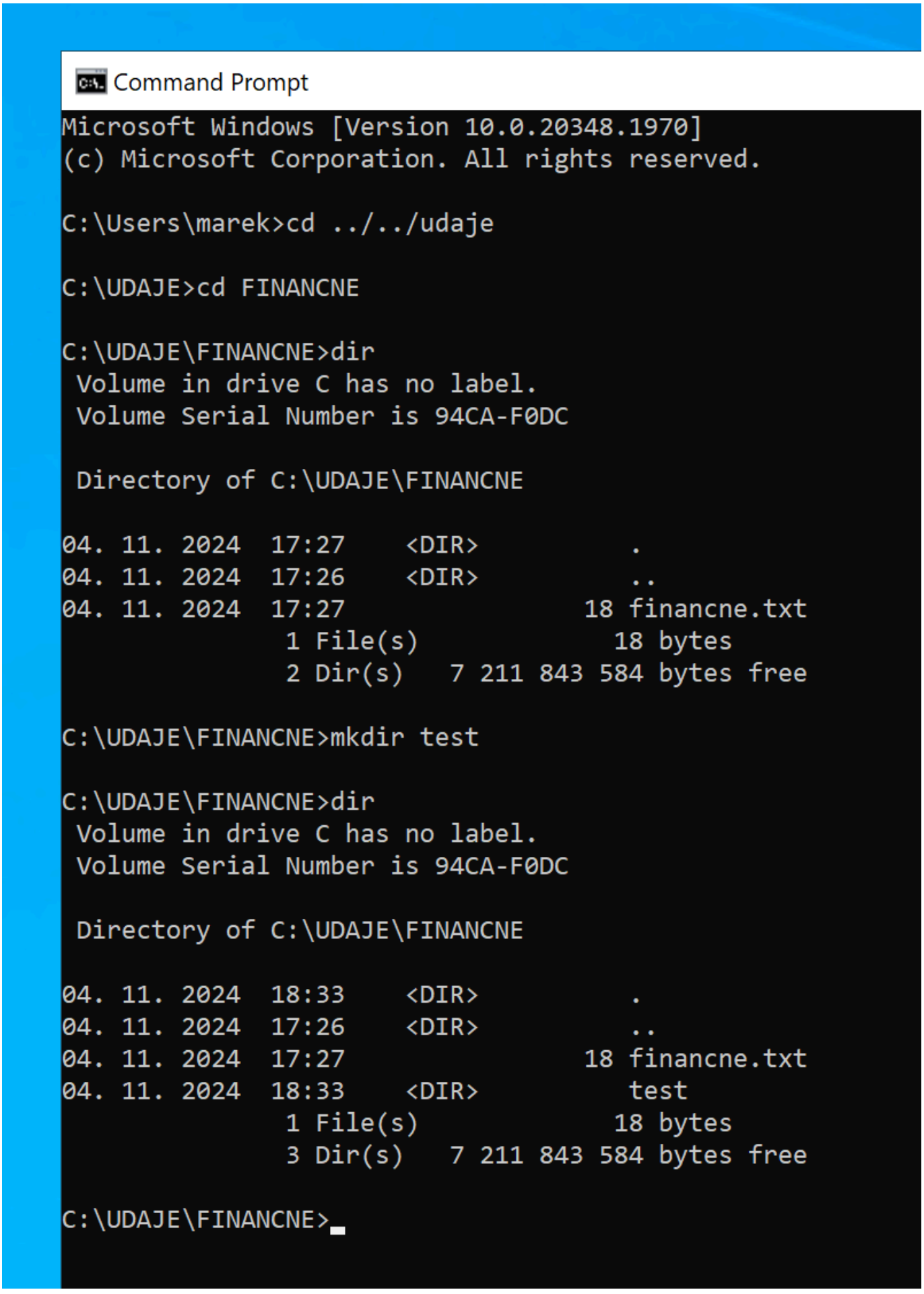
```
C:\Users\user2>cd ../UDAJE
The system cannot find the path specified.

C:\Users\user2>cd ../../UDAJE

C:\UDAJE>ls
'ls' is not recognized as an internal or external command,
operable program or batch file.

C:\UDAJE>dir
 Volume in drive C has no label.
 Volume Serial Number is 94CA-F0DC

 Directory of C:\UDAJE

04. 11. 2024  17:26    <DIR>          .
04. 11. 2024  17:27    <DIR>          FINANCNE
04. 11. 2024  17:29    <DIR>          PERSONALNE
               0 File(s)              0 bytes
               3 Dir(s)   7 177 613 312 bytes free

C:\UDAJE>mkdit test
'mkdit' is not recognized as an internal or external command,
operable program or batch file.

C:\UDAJE>mkdir test
Access is denied.

C:\UDAJE>_
```


Command Prompt
Microsoft Windows [Version 10.0.20348.1970]
(c) Microsoft Corporation. All rights reserved.
C:\Users\marek>whoami
marek0\marek
C:\Users\marek>cd ../../udaje
C:\UDAJE>mkdir test
Access is denied.
C:\UDAJE>

ems

e)


Command Prompt
Microsoft Windows [Version 10.0.20348.1970]
(c) Microsoft Corporation. All rights reserved.
C:\Users\user2>cd ../../udaje
C:\UDAJE>cd PERSONALNE
C:\UDAJE\PERSONALNE>dir
Volume in drive C has no label.
Volume Serial Number is 94CA-F0DC
Directory of C:\UDAJE\PERSONALNE
04. 11. 2024 17:29 <DIR> .
04. 11. 2024 17:26 <DIR> ..
04. 11. 2024 17:29 20 personalne.txt
1 File(s) 20 bytes
2 Dir(s) 7 209 922 560 bytes free
C:\UDAJE\PERSONALNE>mkdir test
C:\UDAJE\PERSONALNE>dir
Volume in drive C has no label.
Volume Serial Number is 94CA-F0DC
Directory of C:\UDAJE\PERSONALNE
04. 11. 2024 18:30 <DIR> .
04. 11. 2024 17:26 <DIR> ..
04. 11. 2024 17:29 20 personalne.txt
04. 11. 2024 18:30 <DIR> test
1 File(s) 20 bytes
3 Dir(s) 7 209 922 560 bytes free
C:\UDAJE\PERSONALNE>


Command Prompt
Microsoft Windows [Version 10.0.20348.1970]
(c) Microsoft Corporation. All rights reserved.
C:\Users\marek>cd ../../udaje
C:\UDAJE>cd FINANCNE
C:\UDAJE\FINANCNE>dir
Volume in drive C has no label.
Volume Serial Number is 94CA-F0DC
Directory of C:\UDAJE\FINANCNE
04. 11. 2024 17:27 <DIR> .
04. 11. 2024 17:26 <DIR> ..
04. 11. 2024 17:27 18 financne.txt
1 File(s) 18 bytes
2 Dir(s) 7 211 843 584 bytes free
C:\UDAJE\FINANCNE>mkdir test
C:\UDAJE\FINANCNE>dir
Volume in drive C has no label.
Volume Serial Number is 94CA-F0DC
Directory of C:\UDAJE\FINANCNE
04. 11. 2024 18:33 <DIR> .
04. 11. 2024 17:26 <DIR> ..
04. 11. 2024 17:27 18 financne.txt
04. 11. 2024 18:33 <DIR> test
1 File(s) 18 bytes
3 Dir(s) 7 211 843 584 bytes free
C:\UDAJE\FINANCNE>

Zadanie č.5

V prípade podnikovej siete možno považovať bránu Firewall servera alebo pracovnej stanice ako poslednú líniu obrany (ak uvažujeme o modeli defense-in-depth).

Všeobecnou úlohou brány firewall je na základe určitých pravidiel povoľovať alebo zakazovať prechod údajov prostredníctvom počítačovej siete. Jej hlavnou úlohou je regulovať tok údajov medzi počítačovými sieťami s rôznymi úrovňami dôvery. Funkciou brány firewall je teda zamedziť prieniku nevyžiadaných údajov z počítačovej siete s nízkou dôverou do počítačovej siete s vyššou dôverou.

Brána firewall systému Windows je navrhnutá na ochranu jediného osobného počítača alebo servera. Prednastavenou konfiguráciou brány firewall je blokovanie všetkej komunikácie smerom z pripojenej počítačovej siete ku klientskej stanici, okrem predvolených služieb, predovšetkým na serveri.

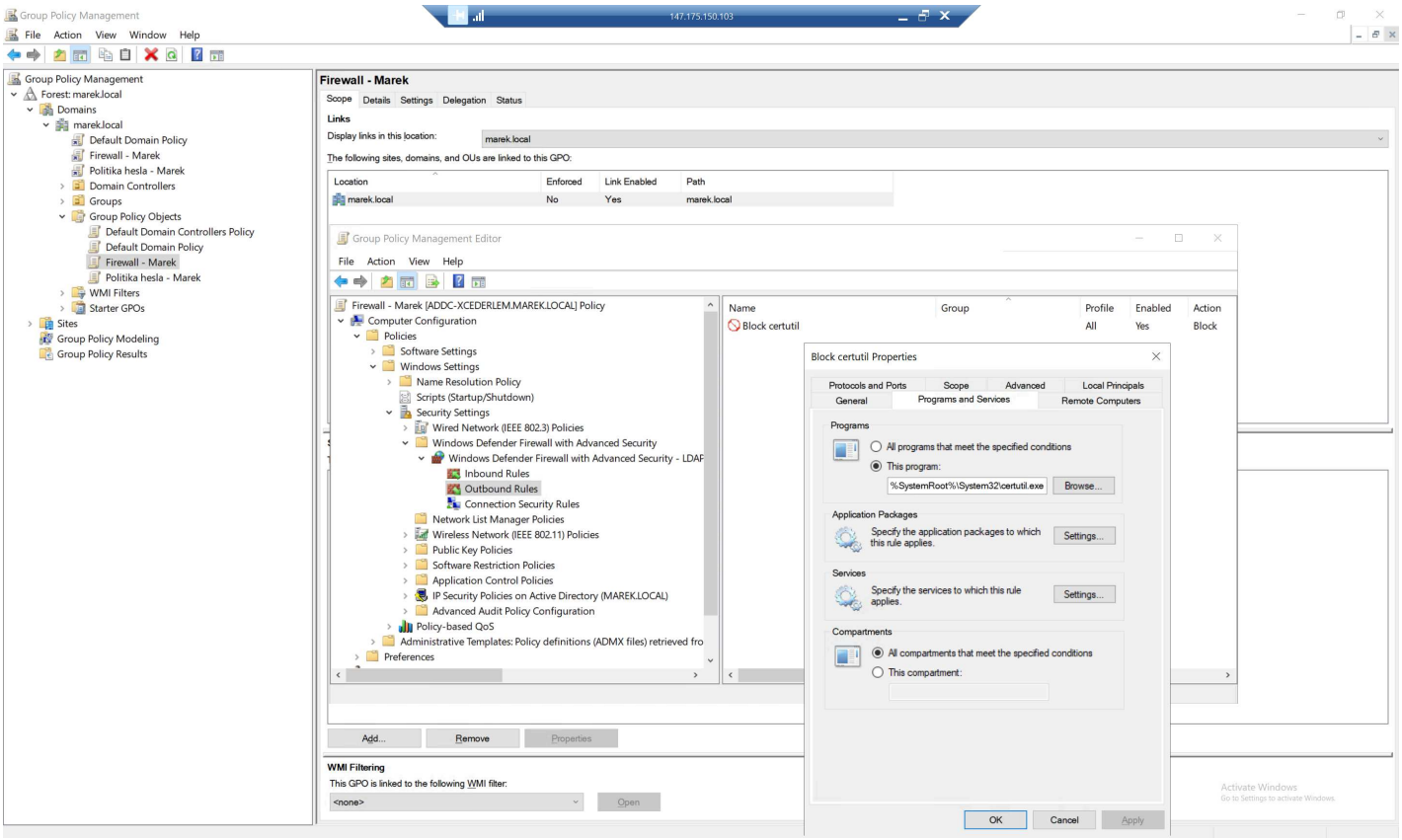
V praxi na Windows Serveri v podnikovom prostredí beží služba DNS, LDAP - kvôli adresárovej službe Active Directory, príp. služba DHCP.

Z používateľského hľadiska je nutné vytvoriť výnimky pre určité aplikácie, ktoré následne brána firewall prepustí zo siete do klientskej stanice.

- Ak útočník kompromituje pracovnú stanicu či server s voľným prístupom k internetu (napr. notebook zamestnanca pracujúceho z domu) má možnosť štandardne komunikovať smerom do internetu pomocou vstavaných nástrojov OS. Útočník môže použiť internetové spojenie na vytváranie zadných vrátok v infraštruktúre alebo ich môže použiť ako riadiaci server,
- **Vašou úlohou** bude prostredníctvom nového objektu skupinovej politiky pomenovaného ako „Firewall – VašeKrstnéMeno“ vytvoriť centrálne pravidlo pre všetky zariadenia v doméne tak, aby sa nemohol legitímny nástroj OS Windows – program certutil pripojiť na internet a stiahnuť do počítača škodlivý súbor.
    - Zistite a stručne (na dva riadky) opíšte ako sa program certutil môže pripojiť do internetu a na čo táto utilita slúži (0,1 b)
    - Vytvorte objekt skupinovej politiky a nastavte blokovanie prístupu tohto programu do internetu (0,4 b)
- Výsledkom má byť na prednáške prezentovaný príklad nastavenia skupinovej politiky.

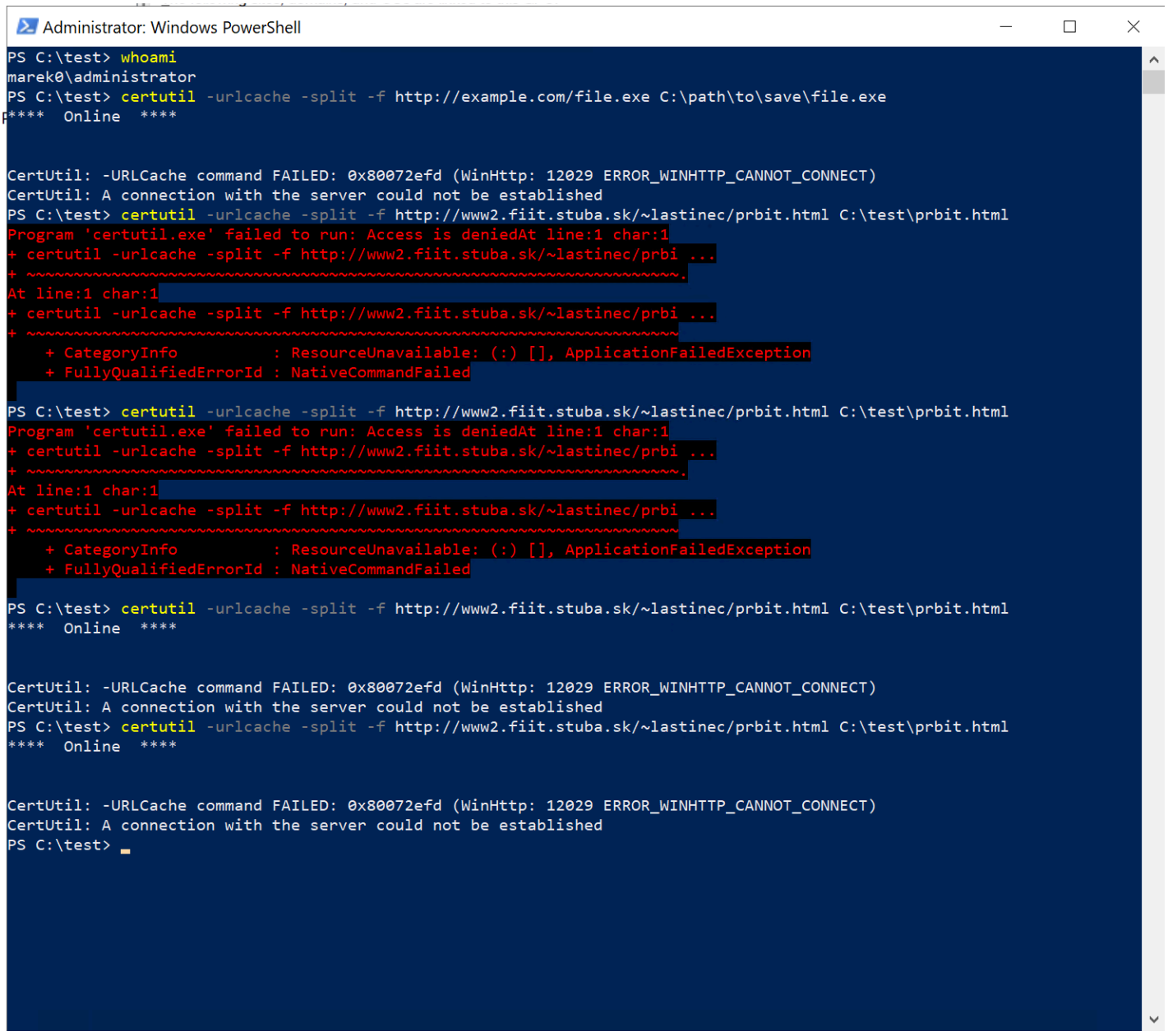
`certutil` je nástroj vo Windowse, ktorý je primárne používaný na správu certifikátov a kľúčov. Vieme ho tiež použiť na sťahovanie súborov cez internet pomocou prepínača `-urlcache`, čo v preklade umožňuje pripojenie na web. Táto funkcia môže byť zneužitá na sťahovanie škodlivých súborov. Kvôli tomuto je vhoďné znemožniť, aby tento program pristupoval na internet.

Vytvorenie nového objektu skupinovej politiky s pravidlom pre zablokovanie prístupu ku `certutil`:



- rovnaké pravidlo som vytvoril aj pre program s cestou `%SystemRoot%\SysWOW64\certutil.exe`, čo je 32-bit verzia programu v adresári, kde sú uložené podporné ovladače pre 32-bit aplikácie
- t.z. zablokovanie pripojenia vo všetkých typoch firewallov

Otestovanie blokovania prístupu k `certutil`:



Červenou farbou je error output, ktorý bol vypísaný kvôli tomu že windows defender zablkovoval vykonanie daného programu pretože ma považoval za útočníka resp. že nejaký trojan sa to snaží vykonať. Po tom, čo som vypol windows defender, tak bol program zablokovaný pomocou pravidla vo firewalle.